Remarks/Arguments

Reconsideration of this application is requested.

Priority

The Action acknowledges applicant's claim for priority but asserts that there is no certified copy of Japanese application No. 2000-092496. This is not understood, because applicant mailed a certified copy of the application to the Office on April 24, 2001. Copies of the Transmittal of Priority document, as well as the return postcard stamped by the OIPE on April 30, 2001 acknowledging receipt of the certified copy of the application, are enclosed. Accordingly, applicant respectfully requests an acknowledgement that all certified copies of priority documents have been received.

Specification Objections

The specification is objected to for various informalities, including typographical and grammatical errors. The informalities noted in the Action are corrected as suggested. In addition, applicant has thoroughly reviewed the specification and has found additional errors which are corrected. No new matter is added.

Claim Status

Claims 1-19 were previously presented. By this amendment, claims 2 and 10 are canceled, and claims 1, 3, 4, 9, 11, 15-17 and 19 are amended. Accordingly, after entry of this amendment, claims 1, 3-9 and 11-19 are pending.

Claim Objections and Rejections under 35 USC 112

The Action objects to informalities in claims 4 and 15 and further rejects claims 1-19 under 35 USC 112, second paragraph, as indefinite. All informalities and indefiniteness issues under 35 USC 112 are corrected.

Claims 1-16 – Rejections under 35 USC 103(a)

Claims 1-16 are rejected under 35 USC 103(a) as obvious over Nishiyama et al. (USP 5,844,691) ("Nishiyama") in view of Barlow (USP 5,204,961) ("Barlow"). Applicant respectfully traverses these rejections. The security system provided by

the present invention is fundamentally different than those shown by Nishiyama and Barlow. In order to clarify this fundamental difference, applicant has amended independent claims 1, 9 and 15.

Nishiyama

Nishiyama, in Figure 16, and in column 17, line 50 to column 18, line 25, describes the delivery of electronic mail to a facsimile and sound serve apparatus 2011. Electronic mail transmitted from an external electronic mail terminal 2214 is transmitted to electronic mail transmitting and receiving portion 2208 via a computer network, such as the Internet. The electronic mail transmitting and receiving portion 2208 sends the received electronic mail to electronic mail registration portion 2207. The electronic mail registration portion 2207 analyzes the electronic mail and converts to have a format matched to the database portion 2203. The converted data is stored in database portion 2203 through database control portion 2202.

Figure 17, and column 18, lines 27-67, describe the transmission of electronic mail from a facsimile and sound serve apparatus 2021. It is simply the operation described in Figure 16 in reverse. Electronic mail conversion portion 2307 reads data stored in data base portion 2303, converts the data into electronic mail format, and transmits the electronic mail to its destination through electronic mail transmission and receiving portion 2308.

Security procedures for incoming electronic mail are described in Fig. 23 and at column 24, lines 27-64. Electronic mail arriving at electronic mail transmission and receiving portion 2908 is sent to registration validation portion 2909, *which checks validation data added to the electronic mail.* The validation data may include data such as passwords, searching data, encoded data and the like. Once validated, the content of the electronic mail is sent to electronic mail registration portion 2907, where it is converted to data base format and sent to data base portion 2903 for storage If the electronic mail is not validated it is abandoned.

Security systems such as Nishiyama that rely on authentication and validation procedures risk exposure to unauthorized access if the validation data attached to the electronic mail (passwords, etc.) is leaked to or obtained by a third party. Once the password or other validation data is in the hands of a hacker or other third party, internal data can be read out or the system can be updated with fraudulent data. The present invention employs a fundamentally different security system that eliminates validation/authentication data and the attendant risk that it will be compromised. Instead, the present invention provides effective protection via one-way communication barriers throughout the system. Data with an external format can be written to received data storage means 6 by server 3, but server 3 cannot read data from received data storage means 6. Similarly, data with an internal format can be read by host computer 10 from received processed data storage means 8, but host computer 10 cannot write data to received processed data storage means 8. Each component of the inventive security system imposes such a one-way communication barrier, and thereby provides effective security without use of authentication data or the like in the vein of Nishiyama.

Independent claims 1, 9 and 15 are amended to clarify this fundamental distinction of the present invention. In claim 1, the received data storage means allows data with an external format received from the server to be written, but prevents data from being read by the server. In Nishiyama, data with an external format is written to electronic mail transmitting and receiving portion 2208, however, there is no disclosure or suggestion that data cannot be read from portion 2208. To the contrary, since element 2208 is identified as an electronic mail *transmitting and receiving* portion, it is clear that data can be written to, and read from, element 2208.

Claim 1 is also amended to require that the received data storage means allows data with an internal format to be read by the host computer, but prevents data from being written by the host computer. In Nishiyama, data with the internal ("database") format is held by data base portion 2203. There is no teaching

or suggestion in Nishiyama that the host computer can read from, but cannot write to, data base portion 2203. All indications in Nishiyama are that the host computer can freely write to and read from base portion 2203. There is no teaching or suggestion of any alternate way of functioning.

Claims 9 and 15 are similarly amended. Claim 9 is directed to security on the transmission side, requiring that the transmit process data storage means allows data with the internal format to be written by the computer, but allows no data to be read by the host computer. The transmit data storage means allows data with an external format to be read by the server but no data may be written by the server. Nishiyama does not disclose or suggest any such "one way" barriers for security. Rather, Nishiyama relies entirely on password-type authentication for security. Claim 15 combines the data reception and transmission aspects of claims 1 and 9.

Barlow

Barlow does not remedy the deficiencies of Nishiyama. Barlow's security system divides computers inside the network into groups called trust regions, having a common security policy in order to protect secrecy of the communication data. Data communication between computers is possible only between computers belonging to the same trust region.

Specifically, a message 153 generated by an initiating application 152 is handed over to a trust realm service program 156 via a network interface 154. Trust realms table 130 is referred to determine whether sending computer 150 and receiving computer 170 belong to the same trust region, and a trust region to perform communication is selected. A trust realm security management system 158 creates a protocol data unit by adding a security label, a sending system, a user, a trust region ID, etc., and a transport service routine 155 sends it. A trust realm service program 174 of the receiving computer 170 refers to a trust realms table 182 to check whether the sending computer 150 and the receiving computer 170 belong to the same trust region. A region security manager 176 performs conversion of the

security label and a permission check and hands over a message 153C to an application via a network interface 184.

Thus, Barlow simply describes a general access restriction method by group management that is reliant on authentication mechanisms. The suggestion at page 7 of the Action that message 153 travels in one direction from network 110 to receiving application 186 bears no relevance to the present invention. Barlow's Figure 3 shows a message traveling in one direction from a sending computer to a receiving computer. This is not the subject matter of the claims of the present invention. The present invention claims a security system in which restrictions on the reading and writing ability of specific transmitting and receiving components establish one way barriers and provide security without need for authentication mechanisms. In claim 1, for example, the received data storage means allows data with an external format received from the server to be written, but prevents data from being read by the server. Similarly, in claim 1, the received data storage means allows data with an internal format to be read by the host computer, but prevents data from being written by the host computer. Barlow contains no such teachings or suggestions and does not remedy the deficiencies of Nishiyama.

For these reasons, claims 1-16 are not rendered obvious by Nishiyama and Barlow. The rejections should be withdrawn.

Claims 17-19 – Rejections under 35 USC 102(b)

Claims 17-19 are rejected under 35 USC 102(b) as anticipated by Nishiyama. Applicant respectfully traverses the rejections, and has amended claims 17-19 to emphasize the distinctive features discussed above.

Independent claims 17 and 19 are directed to the mail transfer section feature of the present invention, in which a mail transfer section has separate mail receiving and sending sections to add an additional level of security. The claims have been amended to emphasize that the mail receiving section can receive mails from, but not send mails to, the mail client. Similarly, the mail sending section can send mails to, but cannot receive mails from the mail server.

In addition, claims 17 and 19 are further amended to emphasize the one way barrier feature discussed above. The host computer can receive data from the mail receiving section but cannot write data to the mail receiving section. Similarly, the host computer can write data to the mail transfer section but cannot read from the mail transfer section.

Nishiyama contains no disclosure or suggestion of these elements, and therefore cannot anticipate claims 17-19. Although Barlow was not relied on in the rejection of these claims, applicant notes that Barlow similarly fails to disclose such one way barriers and is likewise deficient.

Conclusion

This application is now believed to be in condition for allowance. The Examiner is invited to telephone the undersigned to resolve any issues that remain after entry of this amendment. Any fees due with this response may be charged to our Deposit Account No. 50-1314.

Respectfully submitted,
HOGAN & HARTSON L.L.P.

Date: February 4, 2005

By: _____
Troy M. Schmelzer
Registration No. 36,667
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Phone: 213-337-6700
Fax: 213-337-6701